

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

THE BLACK BMW SEDAN BEARING TEXAS
TEMPORARY REGISTRATION 07192E7 AND VIN
3MW5R1J07L8B22698

Case No. 1:22-MJ-00430

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A (incorporated by reference).

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 922(a)(6), 1341, 1343, 1349, 1028A, 371	False Statement During Purchase of a Firearm, Mail Fraud, Wire Fraud, Conspiracy to Commit Mail and Wire Fraud, Aggravated Identity Theft, Conspiracy to Commit an Offense Against the United States

The application is based on these facts:

See Attached Affidavit (incorporated by reference).

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Derek Graham

Applicant's signature

Derek Graham, Special Agent, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
FaceTime Video Conference (specify reliable electronic means).

Date: Jul 20, 2022

City and state: Cincinnati, OH

Stephanie K. Bowman

Judge's signature

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title



ATTACHMENT A

Property to Be Searched

The **TARGET VEHICLE** to be searched is further described as the black BMW sedan bearing Texas temporary registration 07192E7 and VIN 3MW5R1J07L8B22698. The property to be searched includes all compartments, storage areas, and other locations within the vehicle, as well as any packages, parcels, bags, boxes, and other containers within the vehicle.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm), 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1028A (Aggravated Identity Theft), and 371 (Conspiracy to Commit an Offense Against the United States) (collectively, the “Target Offenses”), those violations involving ANEESAH WILLIAMS, NEHEMIAH JONES, ZEPHANIAH JONES, JERIN JOHNSON, SR., and other known and unknown coconspirators and occurring after on or about April 8, 2022, including:

- a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;
- b. Records and information relating to the possession, theft, use, and/or transfer of personally identifiable information and financial information, including but not limited to credit card information;
- c. Records and information relating to the identity of coconspirators to the scheme under investigation;
- d. Records and information relating to preparatory steps taken in furtherance of the scheme to defraud;
- e. Records and information relating to steps taken to evade capture for the Target Offenses;
- f. Records and information relating to communications between any coconspirators involved in the Target Offenses;

- g. Records and information relating to the proceeds of the scheme, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;
 - h. Records and information relating to who has occupancy and control over the premises searched, including but not limited to keys, rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.
- 2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.
- 3. Copies of ATF Forms 4473s, and any related purchase and sale documents and receipts.
- 4. Any U.S. currency in an amount of at least \$100 that constitutes evidence of, or the proceeds of, illegal firearm sales.
- 5. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.
- 6. Keys, paperwork, and other indicia of ownership of, or control over, a black BMW sedan;
- 7. Computers or storage media used as a means to commit the violations described above.
- 8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
THE BLACK BMW SEDAN BEARING
TEXAS TEMPORARY REGISTRATION
07192E7 AND VIN 3MW5R1J07L8B22698

Case No. 1:22-MJ-00430

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Derek Graham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a warrant to search the black BMW sedan bearing Texas temporary registration 07192E7 and VIN 3MW5R1J07L8B22698 (the “**TARGET VEHICLE**”), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), and have been so employed since October of 2007. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator School, located in Brunswick, Georgia. I graduated from the ATF Special Agent Basic Training Academy, located in Brunswick, Georgia, in April 2008. Prior to my employment with ATF, I was a Federal Air Marshal in the Department of Homeland Security from June 2006 through October 2007. In addition, I was a Criminal Research Specialist with the Washington, DC High Intensity Drug Trafficking Area/Drug Enforcement Administration from June 2003 through June 2006. I am a graduate of Augustana College, where I received a Bachelor’s degree in Business Administration in May of 2002. I am also a graduate of Boston University, where I received a master’s degree in Criminal Justice in June of 2006.

3. I have experience in the investigation, apprehension, and prosecution of individuals suspected of being involved in federal firearms and drug offenses. I have specific experience in investigating the use of cell phones by criminal suspects who are involved in the commission of those offenses. I have been trained by ATF as a Digital Media Collection Specialist (DMCS) and have completed more than 285 forensic extractions of cellular telephones, computers, and other electronic storage media. I have also reviewed forensic extractions of cellular telephones, computers, and other electronic storage media, and have examined content and communications contained within these devices obtained by forensic extraction. This content includes records of communication through call logs, text message content, images and videos, and communication made through various social media applications.

4. I know from training and experience that individuals typically keep cell phones in their residences, on their persons, or within their immediate control, such as in the cupholder of a car they are driving, because cell phones are regularly used and possessed as an item of personal property. I also know from my training and experience that in today's age it is typical for individuals engaged in criminal activity to possess multiple active cellular phones at one time. For example, many criminals have one phone that they use for personal communications (e.g., with family members) and another phone that they use to communicate with criminal associates.

5. I also know based on my training and experience and from discussions with other experienced agents and officers that, when individuals are involved in an illegal business, such as firearms trafficking, drug trafficking, and/or the trafficking of stolen financial information, those individuals commonly maintain in their residences (including in short-term residences, such as hotel rooms), on their persons, and/or in their vehicles lists of customers, supplier lists, pay/owe sheets, receipts, address books, financial information, and other documents listing the price and

quantity of items sold, as well as the date the items were purchased, possessed, and sold. These records may be stored in paper form or on electronic devices, such as cell phones and other electronic storage media.

6. Additionally, based on my training and experience, I know that firearms traffickers commonly store in their residences (including in short-term residences, such as hotel rooms) and/or vehicles, as well as carry on their persons, fruits and contraband of their trafficking, such as firearms, ammunition, firearms accessories, and the proceeds of their trafficking. It is also common for individuals to carry on their person or in their vehicles items allowing them to access premises they control, such as house keys and garage-door openers, as well as documentation showing their association with certain premises, such as identification cards and other paperwork listing home addresses.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm), 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1028A (Aggravated Identity Theft), and 371 (Conspiracy to Commit an Offense Against the United States) (collectively, the “Target Offenses”) have been committed by ANEESAH WILLIAMS, ZEPHANIAH JONES, NEHEMIAH JONES, JERIN JOHNSON, SR., and other known and unknown coconspirators. There is also probable cause to search the **TARGET VEHICLE**

described in Attachment A for the evidence, instrumentalities, fruits, and contraband of these crimes further described in Attachment B.

PROBABLE CAUSE

A. ATF and the U.S. Attorney's Office are investigating a fraud scheme in which the perpetrators use stolen credit card information to purchase firearms online and have them shipped to Cincinnati.

9. From on or about April 8, 2022, through on or about June 22, 2022, certain individuals made more than 376 attempts to purchase firearms online and/or to have them transferred by mail to various Federal Firearms Licensees (FFLs) in the Southern District of Ohio, where the transactions could be completed and the firearms could be picked up. Many of these orders were placed in the name of one of the following individuals: ANEESA WILLIAMS, ZEPHANIAH JONES, NEHEMIAH JONES, and JERIN JOHNSON, SR., among others. Many, and possibly all, of the purchases and attempted purchases were made using stolen credit card information.

10. Further investigation has shown that, after some purchases went through, and the firearms were shipped to Cincinnati, some of the suspects named above arrived at FFLs in the Southern District of Ohio and completed, or attempted to complete, the transfers.¹ During some of those in-person interactions, the suspects have represented that they were the true purchasers of the firearms but have made statements or taken other actions suggesting that, in fact, they

¹ Based on my training and experience, I know that a sale of a firearm through an FFL is required to take place in the same State as which the individual is a resident. If an individual purchases a firearm from an FFL from another State, the FFL will transfer the firearm to an FFL within the individual's State of residence. The FFL in the receiving State may then complete the transfer, and finalize the sale, by having the purchasing individual complete an ATF Form 4473. An FFL participating in the final stage of the transfer to the purchasing individual generally charges a nominal fee for the service.

were buying the firearms for someone else. Some of the suspects have also provided false information about their residences on ATF Form 4473 – Firearms Transaction Record (“ATF Form 4473”).

11. I am now seeking a warrant authorizing the search of the **TARGET VEHICLE**, because there is probable cause to believe that it will contain the items described in Attachment B, which are evidence, instrumentalities, fruits, and contraband of violations of the Target Offenses. These items include but are not limited to electronic devices used in furtherance of, or that contain evidence of, the Target Offenses; firearms, ammunition, and firearm paraphernalia; records related to firearms and firearms purchases or transfers; and evidence relating to the possession and use of stolen credit card information.

B. On May 15, 2022, six firearms were purchased online from an FFL in Knoxville, TN, in WILLIAMS’s name, but listing a billing address in Florida.

12. On May 15, 2022, two online orders for a total of six firearms were placed in WILLIAMS’s name with FFL Smoky Mountain Guns & Ammo in Knoxville, TN (“Smoky Mountain Guns”), for transfer to North College Hill Gun Store in Cincinnati.

13. For both orders, WILLIAMS’s address was listed as an address on 88th Ave. North in Pinellas Park, FL. The listed telephone number was 614-XXX-7794,² and the email address was ESSENCED2016@GMAIL.COM. Records from Google, produced in June 2022, show that ESSENCED2016@GMAIL.COM has as its recovery SMS phone number 267-XXX-

² At times in this affidavit I replace digits from phone numbers with “XXX.” The records list the full phone numbers; however, where the full number is not needed for probable cause, I have replaced some digits with “XXX” to minimize the need for redactions if this affidavit is later unsealed. For similar reasons, I have not provided full addresses used on the online orders, particularly since many of these addresses appear to belong to victims of identity theft.

1136—a phone number that was also used for other online orders of firearms placed in the name of NEHEMIAH JONES³; as I describe below, the evidence suggests that these orders were fraudulent and placed as part of the same conspiracy, because they were also paid for using suspected stolen credit card information and false addresses.

14. On May 20, 2022, WILLIAMS arrived at North College Hill Gun Store to complete the transfer. According to employee B.P., WILLIAMS was accompanied by an unknown Black male. According to B.P., the unknown Black male asked about some firearms, prompting B.P. to ask the male’s age. Upon learning that the male was under twenty-one years of age, B.P. said he would not speak with the male about firearms.⁴

15. On the ATF Form 4473 for the transfer of the six firearms, WILLIAMS once again listed an address on Knox Street in Cincinnati—not the Florida address used for the online purchases in her name.

16. In Box 10 of the ATF Form 4473, which asks for the purchaser’s “Current State of Residence and Address,” WILLIAMS started to write and then scratched out “370” and another digit that cannot be fully read, as shown below.

³ This telephone number was also provided by ZEPHANIAH JONES, a suspected coconspirator in the scheme and relative of NEHEMIAH JONES, as discussed in more detail below, on two separate ATF Form 4473s from April 1 and 12, 2022, respectively.

⁴ An FFL is prohibited from transferring handguns to a person under the age of 21. There is no Federal prohibition on speaking with an individual under the age of twenty-one about a handgun, but an FFL may choose to enact this policy at their own discretion.

Section B - Must Be Completed Personally By Transferee/Buyer					
9. Transferee's/Buyer's Full Name (If legal name contains an initial only, record the initial followed by "IO" in quotes. If no middle initial or name, record "NMN".)					
Last Name (including suffix, e.g., Jr, Sr, II, III)		First Name		Middle Name	
Williams		Aneesah		Monet	
10. Current State of Residence and Address (U.S. postal abbreviations are acceptable. Cannot be a post office box.)					
Number and Street Address		City		State	ZIP Code
[REDACTED] Knox St		Cincinnati		OH	45204
County/Parish/Borough		Hamilton			
11. Place of Birth		12. Height	13. Weight	14. Sex	15. Birth Date
U.S. City and State		Ft. 4	(lbs.)	<input type="checkbox"/> Male	Month Day Year
Cincinnati Ohio		In. 9	115	<input checked="" type="checkbox"/> Female	[REDACTED] [REDACTED] 1995
-OR- Foreign Country					

17. I believe WILLIAMS likely started writing "3707 Glenway Ave.," because, among other reasons, from June 9 through mid-July 2022, law enforcement saw ANEESAH WILLIAMS entering and/or exiting that address, and records from Duke Energy show that WILLIAMS is the listed subscriber for utilities at that address.

C. On June 1, 2022, after American Trading denied another attempted purchase by WILLIAMS, an unknown male, via phone, threatened violence against the FFL.

18. On June 1, 2022, WILLIAMS returned to American Trading. Employee N.C. said that, upon entering, WILLIAMS asked if N.C. remembered her and said she was there to pick up "that Glock."

19. N.C. said he/she told WILLIAMS that a firearm had not arrived for her. According to N.C., WILLIAMS became upset and called someone that she identified to N.C. as "[her] man."

20. N.C. asked WILLIAMS where she had purchased the firearm she intended to pick up, and WILLIAMS responded that she had purchased it from FedEx. FedEx is not an FFL, so I believe this statement is evidence that WILLIAMS did not place the order herself.

21. N.C. said he/she told WILLIAMS that she could not purchase a firearm for another person and that American Trading did not want her business if she was doing so. WILLIAMS then left without completing the transfer of a firearm.

22. N.C. said that, approximately five minutes later, an unknown male called American Trading from phone number 330-XXX-0471, referenced WILLIAMS's name, and asked about the firearm WILLIAMS had attempted to obtain. According to N.C., the unknown male called the firearm "my gun" and asked N.C. why he could not have it. According to N.C., the unknown male also said he knew where N.C. was and that he was going to shoot N.C.

23. Another employee, D.P., said the unknown male called again a short time later and asked what time they (the employees) got out of work and asserted that he was going to shoot D.P. and the front of the store.

24. According to D.P., he/she received a telephone call on June 2, 2022, from the transferring FFL regarding the firearm that WILLIAMS had attempted to pick up the day before. D.P. said he/she told the FFL not to transfer the firearm and that he/she would not be completing the transfer to WILLIAMS.

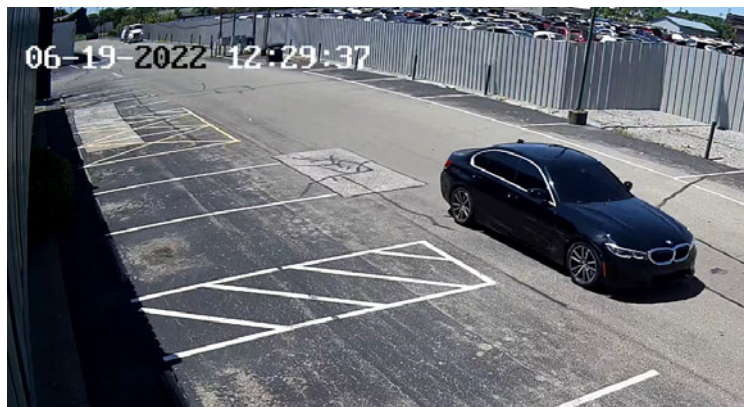
D. Also on June 1, 2022, WILLIAMS completed a transfer of another firearm from North College Hill Gun Store.

25. On the same day as the denied transaction described in the preceding section—June 1, 2022—WILLIAMS completed a transfer of a pistol from North College Hill Gun Store. The firearm had been ordered in her name from Smoky Mountain Guns. On the ATF Form 4473, WILLIAMS listed an address on Knox Street in Cincinnati.

26. According to employee B.P., WILLIAMS said another firearm was being shipped to North College Hill Gun Store and that she would return once it arrived. However, B.P. explained that Smoky Mountain Guns contacted him/her on June 3, 2022, and requested that the firearms not be transferred to WILLIAMS due to being a suspected fraudulent purchase.

E. WILLIAMS arrived at Target World on June 19, 2022, in a black BMW sedan and attempted to complete a transfer of a firearm.

27. On June 19, 2022, ANEESAH WILLIAMS arrived at Target World to complete the transfer of firearms delivered on June 3, 2022. Exterior surveillance video shows that a vehicle, which, based on my experience and familiarity with cars, I recognize as a black four-door BMW sedan, arrived and parked in the parking lot of Target World. (See image below.) WILLIAMS then got out of the front passenger seat of the BMW and went inside.



28. It was not possible to determine the license plate number from the surveillance video; however, based on the information I describe below linking a black BMW sedan to ZEPHANIAH JONES, I submit that there is probable cause to believe that this BMW was the **TARGET VEHICLE** that I am seeking a warrant to search.

29. Target World Sales Associate D.C., who was present that day, said WILLIAMS came into Target World by herself and attempted to complete the transfer of two firearms that had been received by Target World on June 3, 2022. D.C. said he/she told WILLIAMS that Smoky Mountain Guns, the FFL from which WILLIAMS purchased the firearms, had contacted Target World and told them it was a fraudulent purchase. D.C. said he/she also told WILLIAMS that the purchase by WILLIAMS was an attempted “straw” purchase.

30. According to D.C., WILLIAMS claimed she had used her own credit card to complete the purchase and acted surprised when told the purchase was fraudulent. D.C. also said that, as WILLIAMS was leaving the store at the end of the encounter, D.C. heard her say, “Those two ratting-ass snitches.” Exterior surveillance video shows that WILLIAMS then got back into the front passenger seat of the black BMW sedan and departed.

F. JERIN JOHNSON, SR. and NEHEMIAH JONES are coconspirators of WILLIAMS’s; they completed a straw purchase on July 6, 2022, at which time ZEPHANIAH JONES was driving a black BMW sedan.

31. Surveillance video shows that, a couple of weeks later, on July 6, 2022, a Black male, later identified as JERIN JOHNSON SR. based on a Form 4473 he filled out, arrived at Target World operating a black four-door sedan, with identifying characteristics of being a Volkswagen-manufactured vehicle (the “Volkswagen”). (See below.)



32. A separate exterior camera angle shows that, at approximately the same time, a black four-door BMW sedan arrived and parked in a separate area of the parking lot. (See zoomed-in screenshot below.) Although the surveillance footage does not permit a comparison of license plates, this vehicle appears to be the same black BMW sedan involved WILLIAMS’s attempted transfer of firearms on June 19, 2022.



33. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Based on this information and the information I describe below linking the **TARGET VEHICLE** to ZEPHANIAH JONES, I submit that there is probable cause to believe that the black BMW sedan seen at Target World on July 6, 2022, was the **TARGET VEHICLE** I am seeking authorization to search.

34. Exterior and interior video show that JOHNSON entered Target World and came out about three minutes later without having completed the transfer of a firearm. JOHNSON then reentered the Volkswagen and drove toward where the black BMW was parked. JOHNSON then appeared to roll his driver's side front window down, and he parked the Volkswagen next to the BMW so that the two driver's windows were facing each other, as pictured below. Based on my training and experience, I know that by orienting two cars in this manner, the drivers of both cars can speak to each other through their driver's side windows.



35. After approximately thirty seconds, JOHNSON backed out of the parking spot and drove away. The BMW waited for a passing vehicle to cross and then drove away in the same direction.

36. About twelve minutes later, JOHNSON returned to Target World in what appears to be the same Volkswagen, parked, and went inside.

37. Surveillance video shows that, while JOHNSON was inside, what appears to be the same black BMW came back and parked in the same parking spot where it had been twelve minutes earlier.

38. Approximately twenty minutes after that, JOHNSON came out of Target World carrying two items. ATF Form 4473s completed by JOHNSON show that he had completed the transfer of two firearms. Video surveillance then shows JOHNSON moving to the area of the rear passenger seat of the Volkswagen, where, based on the later behavior I describe below, I believe he placed the firearms. JOHNSON then returned to the driver's seat and pulled out of the parking spot.

39. Surveillance footage shows that, about twenty-five seconds later, JOHNSON parked the Volkswagen in a backwards orientation next to the BMW. JOHNSON then got out of the Volkswagen and opened its rear passenger door. The video then appears to show JOHNSON interacting with the rear driver's door of the other vehicle. Based on this footage, the broader

context of the straw purchasing scheme described in this affidavit, and my training and experience, I believe JOHNSON placed the firearms he had purchased from Target World into the back seat of the BMW. The video then appears to show JOHNSON moving slightly towards the front of the other vehicle, suggesting he was meeting with the driver of the other vehicle.

40. About fifteen seconds later, the BMW drove away, and JOHNSON then returned to his car and departed.

41. [REDACTED]

[REDACTED]

[REDACTED]

42. The ATF Form 4473 completed by JOHNSON on July 6, 2022, shows that he listed telephone number 513-XXX-1462 as his contact phone. This same phone number was listed on an ATF Form 4473 from North College Hill Gun Shop related to a firearm transfer by ZEPHANIAH JONES on or about June 14, 2022.

43. Records from Guns.com show forty-seven attempted firearms purchases in the name of JERIN JOHNSON SR. in just three days, from June 20, 2022, to June 22, 2022. Each of these attempted purchases appears to have been placed with fraudulent credit card information. For example, five different billing addresses were used. JOHNSON arrived at Cincinnati-area FFLs to complete some of these transfers on June 24, June 28, July 6, and July 8, 2022.

44. Records from Guns.com show that the purchases in JOHNSON's name were placed from IP address 52.124.36.227, which is also associated with attempted firearm purchases in the names of ANEESAH WILLIAMS, Dewayna Stevens, Kashawna Fisher, Kiana Harrell, Mykia Melton, NEHEMIAH JONES, and ZEPHANIAH JONES. As I describe in more detail below, this IP address is linked to a residence used by NEHEMIAH and ZEPHANIAH JONES.

G. IP information links the fraudulent purchases in WILLIAMS's name to fraudulent purchases in the names of several others, including NEHEMIAH and ZEPHANIAH JONES, who have completed some of the transfers in person.

45. Records from Guns.com show that the approximately 67 online orders placed in WILLIAMS's name, all using suspected stolen credit card information, were placed from IP address 52.124.36.227, and that many more attempted orders were placed in the names of other individuals from that same IP. Relevant details of some of those other orders are as follows:

Name	Date(s)	Attempts	Email(s)	Billing Address(es)
Mykia Melton	5/25 – 5/26/22	37	RAYNELLPARKS@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Smiley Ave West lake OH, 44145 • [Redacted] Gatehouse Lane Columbus OH, 43235 • [Redacted] West Exchange Street Akron OH, 44313 • [Redacted] Saint Andrews Drive Westerville OH, 43082 • [Redacted] Maplebrooke Drive East Westerville OH, 43082 • [Redacted] East High Street Mantua OH, 44255
Kiana Harrell	5/27- 5/28/22	39	RAYNELLJONES80@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Greenoak Dr Cincinnati OH, 45248 • [Redacted] Warrensburg Road Delaware OH, 43015 • [Redacted] Kennard Road Medina OH, 44256 • [Redacted] Crary Lane Willoughby OH, 44094 • [Redacted] E Lincoln Highway Lima OH, 45807 • [Redacted] Wickcliffe Road Columbus OH, 43221 • [Redacted] Niderdale Way Middletown OH, 45042
NEHEMIAH JONES	5/30- 6/3/22	22	NEHEMIAHJ470@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Niderdale Way Middletown OH, 45042 • [Redacted] Windward Circle Aurora OH, 44202 • [Redacted] Lightwind Court Westerville OH, 43081 • [Redacted] Woodstock Drive Avon Lake OH, 44012

				<ul style="list-style-type: none"> • [Redacted] Franks Road Southeast Heath OH, 43056 • [Redacted] Beachview Road Willoughby OH, 44094 • [Redacted] Kinsman Court Columbus OH, 43207
NEHEMIAH JONES	4/8-4/23/22	7	SPEEDKILLER2108@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Parkside Drive Parma OH, 44130 • [Redacted] Morse rd columbus OH, 43230 • [Redacted] Glenwood Dr Twinsburg OH, 44087 • [Redacted] Glen Allen Drive Cleveland Heights OH, 44121
JERIN JOHNSON SR.	6/20-6/22/22	47	OFFICIALK2163@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Public Square Cleveland OH, 44113 • [Redacted] Mc Intosh Road Pataskala OH, 43062 • [Redacted] Public Square Cleveland OH, 44113 • [Redacted] Township Road 162 Cardington OH, 43315 • [Redacted] 2nd Street Clarksville OH, 45113 • [Redacted] Holloway Rd Holland OH, 43528
Kashawna Fisher	4/22 – 4/28/22	26	DJOMKAMALVINEE@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Northfield Court Springfield OH, 45502 • [Redacted] Southwood Drive Lima OH, 45805 • [Redacted] Northfield Court Springfield OH, 45502 • [Redacted] Croydon Drive Northwest Canton OH, 44718 • [Redacted] Northfield Court Springfield OH, 45502 • [Redacted] Tanbark Lane Strongsville OH, 44149
ZEPHANIAH JONES ⁵	4/10-4/22/22	6	ZEPH21J@ICLOUD.COM	<ul style="list-style-type: none"> • [Redacted] Shepherds Way Batavia OH, 45103 • O'Bryan Place Centerville OH, 45459

⁵ A query in OHLEG, a database available to law enforcement, showed that NEHEMIAH JONES and ZEPHANIAH JONES were issued Ohio Identification Cards with the same home address on them. This leads me to believe that the two are relatives, possibly brothers.

				<ul style="list-style-type: none"> • [Redacted] Dover Center Road Bay Village OH, 44140 • [Redacted] Walden Glen Circle Cincinnati OH, 45231 • [Redacted] Dill Road Cleveland OH, 44121
Dewayna Stevens	4/11/22	4	MARYVENO1937@GMAIL.COM	<ul style="list-style-type: none"> • [Redacted] Tara Boulevard Jonesboro GA, 30236 • [Redacted] Ellis Street Metter GA, 30439 • [Redacted] Newcastle Circle Stonecrest GA, 30038

46. Both ZEPHANIAH JONES and NEHEMIAH JONES have arrived at Cincinnati-area FFLs to complete some of these firearms transfers of firearms purchased with suspected stolen credit card information. Specifically, NEHEMIAH JONES completed at least two transfers, and ZEPHANIAH JONES completed transfers of at least seven firearms between April 1 and July 12, 2022.

H. IP information provides further evidence of links among the coconspirators and links the purchases to a residence used by ZEPHANIAH JONES and NEHEMIAH JONES.

47. IP address 52.124.36.227 is linked to approximately 255 attempted firearms purchases between April 8 and June 4, 2022, associated with the following email addresses: ANEESAHW1994@GMAIL.COM, ANEESAHWILLIAMS10@GMAIL.COM, CLEARY091150@GMAIL.COM, MARYVENO1937@GMAIL.COM, DJOMKAMALVINEE@GMAIL.COM, NEHEMIAHJ470@GMAIL.COM, RAYNELLJONES80@GMAIL.COM, RAYNELLPARKS@G-MAIL.COM, OFFICIALK2163@GMAIL.COM, SPEEDKILLER2108@GMAIL.COM, and ZEPH21J@ICLOUD.COM.

48. Records from internet service provider Whitesky Communications show that the above-described IP address 52.124.36.227, is used to provide service to the housing complex at 424 Straight Street, Cincinnati, OH, which is an apartment building at which NEHEMIAH JONES and ZEPHANIAH JONES are registered tenants.

I. There is probable cause to believe that ZEPHANIAH JONES drives the TARGET VEHICLE.

49. On July 19, 2022, pursuant to a federal search warrant, fixed-interval location monitoring was started on a telephone number used by ZEPHANIAH JONES. From approximately 8:05pm to 9:50pm, fixed-interval location information identified the device as being in the approximate area of the Aloft Hotel at 201 3rd St, Newport, KY 41071 (the “Aloft”).

50. At approximately 8:27pm on July 19, 2022, ATF Task Force Officer (TFO) Joseph Ruchti saw a black BMW sedan bearing Texas temporary registration 07192E7 (i.e., the **TARGET VEHICLE**) in the parking garage of the Aloft. This vehicle matched the description of the black BMW seen on surveillance video from Target World on June 19 and July 6, 2022. Law enforcement queried the temporary registration and determined the registration to be fictitious.

51. SA Scott reviewed a Facebook account that, based on the photos posted to it, appeared to belong to ZEPHANIAH JONES. SA Scott saw that, on April 23, 2021, a photo was posted to the account that appeared to depict ZEPHANIAH JONES posing next to a black BMW sedan matching the description of the **TARGET VEHICLE**. (See below.)



52. ATF TFO Ruchti reviewed the VIN listed on the temporary tag for the **TARGET VEHICLE** and compared it to the VIN on the vehicle itself; the VINs matched. SA Scott then ran a query on the VIN for the **TARGET VEHICLE** in a reliable database used by law enforcement and found that title for the vehicle had been transferred to Carvana LLC in Columbus, Ohio, on or about April 21, 2021—two days before the above-described Facebook photo was posted. Based on this information, I believe ZEPHANIAH JONES has had possession or control of the **TARGET VEHICLE** since approximately April 23, 2021.

53. At approximately 10:00pm on July 19, 2022, TFO Ruchti saw the **TARGET VEHICLE** depart from the parking garage of the Aloft being operated by a Black male.

54. As noted above, from about 8:05 pm to 9:50pm, fixed-interval location information identified ZEPHANIAH JONES's phone as being in the approximate location of the Aloft. The next location "ping" received, at approximately 10:06pm that night, showed that the

device was then near the intersection of Plum Street and West Ninth in Cincinnati. Based on this location information and the surveillance showing the black BMW departing the Aloft at about 10:00pm, I submit that there is probable cause to believe that ZEPHANIAH JONES's cell phone was inside the **TARGET VEHICLE** and that ZEPHANIAH JONES was driving the vehicle.

55. At approximately 10:30pm, Newport Police Department Sgt. Adam Moeves entered the Aloft and requested a copy of the guest registry. Sgt. Moeves gave the list to ATF SA John Scott, who found "JERIN JOHNSON, SR." as a name on the guest registry, assigned to room 511 of the Aloft. The records showed that the room had been rented in JERIN JOHNSON, SR.'s name since July 18, 2022, and that the expected departure date was July 21, 2022.

56. In the early morning on July 20, 2022, fixed-interval location monitoring again placed ZEPHANIAH JONES's phone in the approximate location of the Aloft. At approximately 6:15am, law enforcement used a cell-site simulator to determine with greater accuracy where ZEPHANIAH JONES's phone was. This investigation showed that the device was in the approximate area of Aloft Room 511.

57. [REDACTED]

[REDACTED]

[REDACTED]

58. Later on July 20, 2022, law enforcement attempted to conduct a traffic stop on the **TARGET VEHICLE**. When a marked police vehicle activated its lights and sirens, the driver of the **TARGET VEHICLE** fled in the **TARGET VEHICLE**.

59. Shortly thereafter, law enforcement found the **TARGET VEHICLE** abandoned on a public road in Cincinnati.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

60. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **TARGET VEHICLE**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

61. *Probable cause.* I submit that if a computer or storage medium is found in the **TARGET VEHICLE**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

C. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

62. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET VEHICLE** because:

A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- B. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpatng the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that

log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- C. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- D. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- E. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

63. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either

seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- A. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- B. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

C. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

64. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

65. Because several people may use the **TARGET VEHICLE**, it is possible that it will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

66. I submit that this affidavit supports probable cause for a warrant to search the **TARGET VEHICLE** described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

67. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of

the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Derek Graham

DEREK GRAHAM

Special Agent

Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and sworn to before me via FaceTime videoconference on July 20, 2022.

Stephanie K. Bowman

HON. STEPHANIE K. BOWMAN

UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to Be Searched

The **TARGET VEHICLE** to be searched is further described as the black BMW sedan bearing Texas temporary registration 07192E7 and VIN 3MW5R1J07L8B22698. The property to be searched includes all compartments, storage areas, and other locations within the vehicle, as well as any packages, parcels, bags, boxes, and other containers within the vehicle.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 922(a)(6) (False Statement During Purchase of a Firearm), 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1028A (Aggravated Identity Theft), and 371 (Conspiracy to Commit an Offense Against the United States) (collectively, the “Target Offenses”), those violations involving ANEESAH WILLIAMS, NEHEMIAH JONES, ZEPHANIAH JONES, JERIN JOHNSON, SR., and other known and unknown coconspirators and occurring after on or about April 8, 2022, including:

- a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;
- b. Records and information relating to the possession, theft, use, and/or transfer of personally identifiable information and financial information, including but not limited to credit card information;
- c. Records and information relating to the identity of coconspirators to the scheme under investigation;
- d. Records and information relating to preparatory steps taken in furtherance of the scheme to defraud;
- e. Records and information relating to steps taken to evade capture for the Target Offenses;
- f. Records and information relating to communications between any coconspirators involved in the Target Offenses;

- g. Records and information relating to the proceeds of the scheme, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;
 - h. Records and information relating to who has occupancy and control over the premises searched, including but not limited to keys, rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.
- 2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.
- 3. Copies of ATF Forms 4473s, and any related purchase and sale documents and receipts.
- 4. Any U.S. currency in an amount of at least \$100 that constitutes evidence of, or the proceeds of, illegal firearm sales.
- 5. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.
- 6. Keys, paperwork, and other indicia of ownership of, or control over, a black BMW sedan;
- 7. Computers or storage media used as a means to commit the violations described above.
- 8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.